

**IN THE UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT**

CINDY ROUGEAU, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

AETNA INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Cindy Rougeau, individually and on behalf of all others similarly situated, brings this action against Aetna, Inc. (“Aetna”). The following allegations are based on Plaintiff’s knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Aetna responsible for the injuries Aetna inflicted on Plaintiff and approximately 3,000,000¹ similarly situated persons (“Class Members”) due to Aetna’s impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the “Data Breach” or “Breach”) between January 28, 2023 and January 30, 2023.² Upon information and belief, the cybercriminals who perpetrated the Breach is a Russian-linked hacker/ransomware group responsible for numerous other hacking events.³

¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 5, 2023).

² <https://apps.web.maine.gov/online/aevviewer/ME/40/0461b276-a513-41ae-a587-c06c971a7d9b.shtml>.

³ <https://www.scmagazine.com/news/ransomware/clop-ransomware-hack-of-fortra-goanywhere-mft-hits-1m-chs-patients> (last accessed on April 5, 2023); <https://www.aha.org/news/headline/2023-02-23-hhs-russia-linked-ransomware-group-claims-continued-health-care-attacks> (last accessed on April 5, 2023).

2. The data that Aetna caused to be exfiltrated by cybercriminals were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information (“PII”) like individuals’ names, addresses, dates of birth, member identification numbers, date of health plan coverage, Social Security numbers, and/or employer names.

3. Upon information and belief, prior to and through the date of the Data Breach, Aetna obtained Plaintiff’s and Class Members’ PII and PHI and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, Aetna inadequately maintained its network, platform, software, and technology partners—rendering these easy prey for cybercriminals.

4. Upon information and belief, the risk of the Data Breach was known to Aetna. Thus, Aetna was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

5. Then, after the Data Breach, Aetna failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, Aetna deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Aetna impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

6. Even when Aetna finally notified Plaintiff and Class Members of their PII and PHI’s exfiltration, Aetna failed to adequately describe the Data Breach and its effects.

7. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of Aetna’s negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

8. Armed with the PII and PHI stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

9. And Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII and PHI, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII and PHI were exfiltrated and compromised in the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Aetna's data security systems, future annual audits, and adequate credit monitoring services funded by Aetna.

PARTIES

13. Plaintiff Cindy Rougeau is a natural person and resident and citizen of the State of New York. Plaintiff Rougeau has no intention of moving to a different state in the immediate future.

14. Defendant Aetna Holdings, LLC is a Pennsylvania corporation with its principle place of business in Hartford, Connecticut.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than that of Aetna.

16. This Court has general personal jurisdiction over Aetna because Aetna's principal place of business and headquarters is in this District. Aetna also regularly conducts substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Aetna conducts substantial business in this District.

FACTUAL ALLEGATIONS

Aetna Collected and Stored the PII and PHI of Plaintiff and Class Members

18. Founded in 1982 as United States Health Care Systems, Inc., Aetna provides medical, pharmacy, dental, behavioral health, group life, disability, and health care management services to patients in the United States.⁴

19. Upon information and belief, Aetna received and maintained the PII and PHI of patients and employees of its clients, such as individuals' names, addresses, dates of birth, member identification numbers, date of health plan coverage, and/or employer names. These records are stored on Aetna's computer systems.

20. Upon information and belief, Aetna (through NationsBenefits Holdings, LLC⁵) used Fortra, LLC ("Fortra") for information technology management and software services, including Fortra's file transfer platform, GoAnywhere MFT. Within this relationship, Aetna entrusted data, including Plaintiff's and Class Members PII and PHI to Fortra.

21. On February 1, 2023, Fortra, LLC disclosed to its customers that its file transfer platform, GoAnywhere MFT, had been hacked, resulting in the exfiltration of customer PII and PHI, including Plaintiff's and Class Members PII and PHI. Aetna then reported that it was one of the affected customers whom Fortra had notified.

22. Because of the highly sensitive and personal nature of the information Aetna acquire and store, Aetna knew or reasonably should have known that it stored protected PII and PHI and must comply with healthcare industry standards related to data security and all federal

⁴ <https://www.sec.gov/Archives/edgar/data/1122304/000095012302001877/y57196e10-k405.htm> (last visited May 12, 2023); <https://www.bloomberg.com/profile/company/AET:US#xj4y7vzkg> (last visited May 12, 2023).

⁵ <https://www.nationsbenefits.com/about-us> (last visited may 5, 2023) (NationsBenefits provides supplemental benefits administration services to several employer and other entities' health plans).

and state laws protecting customers' and patients' PII and PHI, and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

23. When Aetna collects this sensitive information, it promises to use reasonable measures to safeguard the PII and PHI from theft and misuse.

24. Aetna acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII and PHI.

25. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII and PHI, Aetna assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

26. On Aetna's website, Aetna promises to only share Plaintiff's and Class Members' PII and PHI in limited circumstances, none of which includes sharing such information with hackers.⁶

27. On Aetna's website, Aetna promises to "use administrative, technical and physical safeguards to keep your information from unauthorized access, and other threats and hazards to its security and integrity. We comply with all state and federal laws that apply related to the security and confidentiality of your PHI."⁷

28. Upon information and belief, Aetna represented to its clients orally and in written contracts, marketing materials, and otherwise that it would properly protect all PII and PHI it obtained. Upon information and belief, Aetna knew or reasonably should have known that such

⁶ <https://www.aetna.com/document-library/legal-notices/documents/health-notice-of-privacy-practices.pdf> (last visited May 12, 2023).

⁷ *Id.*

representations would be passed on to its clients' health plan members, including Plaintiff and Class Members.

29. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

30. Upon information and belief, Plaintiff and Class Members relied on Aetna to keep their PII and PHI confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

31. Aetna could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting and supervising its information technology partners.

32. Aetna's negligence in safeguarding Plaintiff's and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

33. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.⁸ Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.⁹

⁸ *2020 Healthcare Data Breach Report*, HIPAA JOURNAL (Jan. 19, 2021) <https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/>.

⁹ *April 2021 Healthcare Data Breach Report*, HIPAA JOURNAL (May 18, 2021) <https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/>.

34. In the context of data breaches, healthcare is “by far the most affected industry sector.”¹⁰ Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.¹¹ And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹²

35. Despite the prevalence of public announcements of data breaches and data security compromises, Aetna failed to take appropriate steps to protect Plaintiff’s and Class Members’ PII and PHI from being compromised.

36. Aetna failed to properly select its information security partners.

37. Aetna failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

38. Aetna failed to ensure the proper monitoring and logging of file access and modifications.

39. Aetna failed to ensure the proper training of its and its technology partners’ employees as to cybersecurity best practices.

40. Aetna failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members.

41. Aetna failed to timely and accurately disclose that Plaintiff’s and Class Members’ PII and PHI had been improperly acquired or accessed.

¹⁰ Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches>.

¹¹ *See id.*

¹² *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

42. Aetna knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI.

43. Aetna failed to provide adequate supervision and oversight of the PII and PHI with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and PHI of Plaintiff and Class Members, misuse the PHI/PII and potentially disclose it to others without consent.

44. Upon information and belief, Aetna failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

45. Upon information and belief, Aetna failed to ensure the proper encryption of Plaintiff's and Class Members' PII and PHI and monitor user behavior and activity to identify possible threats.

The Data Breach

46. On or about April of 2023, Aetna notified the public ("Notice of Data Breach" or "Notice") that its customers' data had been compromised in a Data Breach suffered by Fortra, and informed them of the following:

NationsBenefits Holding, LLC, and its affiliates and subsidiaries (collectively, "NationsBenefits" or "we"), provides benefits administration services to your health insurer, Aetna. We place a high value on maintaining the privacy and security of the information we maintain for our health plan customers. Regrettably, this letter is to inform you that a vendor we used to exchange files with Aetna was recently the victim of a cybersecurity attack, which impacted some of your personal information. We notified Aetna of this incident on February 9, 2023. This letter explains the incident, the measures we have taken in response and the steps you can take.

What Happened? NationsBenefits used software provided by a third-party vendor, Fortra, LLC ("Fortra"), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and

launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our investigation, NationsBenefits analyzed the impacted data to determine whether any individual's personal information was subject to unauthorized access or acquisition. On February 23, 2023, NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.

47. Upon information and belief, the Notice of Data Breach was drafted and publicized under the direction of NationsBenefits Holding, LLC, Fortra, and Aetna.

48. Although the Data Breach began on January 28, 2023, it was not until January 30, 2021—two days later—that Fortra became aware of suspicious activity on their network.

49. Upon information and belief, Plaintiff's and Class Members' PII and PHI was access, exfiltrated, and stolen in the Breach by a Russian linked hacker/ransomware group.¹³

50. Upon information and belief, the Data Breach affected over 130 organizations that use Fortra's file transfer platform called GoAnywhere.¹⁴

51. Upon information and belief, Aetna has sufficient control over Fortra's file transfer platform GoAnywhere to properly secure Aetna's data that is sent over GoAnywhere.

52. Upon information and belief, Fortra's file transfer platform GoAnywhere is partially or fully maintained and hosted on Fortra's own network.¹⁵

53. Upon information and belief, Plaintiff's and Class Members' affected PII and PHI was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

¹³ <https://www.scmagazine.com/news/ransomware/clop-ransomware-hack-of-fortra-goanywhere-mft-hits-1m-chs-patients> (last accessed on April 5, 2023); <https://www.aha.org/news/headline/2023-02-23-hhs-russia-linked-ransomware-group-claims-continued-health-care-attacks> (last accessed on April 5, 2023).

¹⁴ *Id.*

¹⁵ https://www.goanywhere.com/?code=CMP-0000002095&ls=717710011&utm_term=fortra%20goanywhere&utm_campaign=Brand+Search+Global%2BE&utm_source=adwords&utm_medium=ppc&hsa_acc=7887499888&hsa_cam=16466321209&hsa_grp=135712580764&hsa_ad=488204485843&hsa_src=g&hsa_tgt=kwd-1956017997300&hsa_kw=fortra%20goanywhere&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwuLShBhC_ARIsAFod4fLIy63LJVldjwIajE5iD96oGqaTbA-yyDmML273CfUeLHVZe9uTsaAiAPEALw_wcB (last accessed on April 5, 2023).

54. It is likely the Data Breach was targeted at Fortra due to its status as large information technology provider to healthcare providers and other businesses that collect, create, and maintain both PII and PHI.

55. While Aetna claims to have become aware of the Breach as early as February 9, 2023, Aetna did not begin notifying some victims of the Data Breach until April of 2023—almost three months later.

56. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

57. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Aetna advised impacted individuals to “remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity” and to follow the below steps to further protect themselves:

- a. order your free credit report;
- b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your state’s attorney general office about for information on how to prevent or avoid identity theft;

- c. place a security freeze; and
- d. place a fraud alert.¹⁶

58. Aetna largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

59. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.¹⁷

60. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;¹⁸ leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"¹⁹ Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

¹⁶ <https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-187.pdf>.

¹⁷ *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS <https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour> (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make \$1,253 per 40-hour work week.).

¹⁸ Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC <https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html> (Nov. 6, 2019).

¹⁹ *Id.*

61. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

62. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII and PHI with the intent of engaging in misuse of the PII and PHI, including marketing and selling Plaintiff's and Class Members' PII and PHI.

63. Aetna also offered credit monitoring services to some Class Members for a period of 24 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

64. Aetna had and continues to have obligations created by HIPAA, reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII and PHI confidential and to protect such PII and PHI from unauthorized access.

65. Aetna's Breach Notice letter, as well as its website notice, both omit the size and scope of the breach. Aetna has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

66. Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being taken, if any, to secure their PII and PHI and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Aetna

intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

67. Plaintiff's and Class Members' PII and PHI and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and PHI and/or financial information of Plaintiff and Class Members.

Aetna Failed to Comply with FTC Guidelines

68. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.²⁰ To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Aetna, should employ to protect against the unlawful exfiltration of PII and PHI.

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.²¹ The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

²⁰ *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), <https://bit.ly/3uSoYWF> (last accessed July 25, 2022).

²¹ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), <https://bit.ly/3u9mzre> (last accessed July 25, 2022).

70. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

71. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.²²

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. These FTC enforcement actions include actions against healthcare providers and partners like Aetna. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[t]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act”).

74. Aetna’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

²² *See Start with Security*, *supra* note 46.

Aetna Failed to Follow Industry Standards

75. Despite its alleged commitments to securing sensitive patient data, Aetna does not follow industry standard practices in securing patients' PII and PHI.

76. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

77. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Aetna, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

79. Aetna failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. Such frameworks are the existing and applicable industry standards in the

healthcare industry. And Aetna failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

Aetna Violated HIPAA

81. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.²³

82. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.²⁴

83. The Data Breach itself resulted from a combination of inadequacies showing Aetna failed to comply with safeguards mandated by HIPAA. Aetna's security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

²³ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

²⁴ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

d. Failing to ensure compliance with HIPAA security standards by Aetna's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

84. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrates Aetna failed to comply with safeguards mandated by HIPAA regulations.

The Experiences and Injuries of Plaintiff and Class Members

85. Plaintiff and Class Members are members of health plans who use Aetna for delivering health services.

86. As a prerequisite of receiving treatment, Aetna requires its customers' health plan members—like Plaintiff and Class Members—to disclose their PII and PHI.

87. When Aetna finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Aetna's Breach Notice sent to patients fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

88. Because of the Data Breach, Aetna inflicted injuries upon Plaintiff and Class Members. And yet, Aetna has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

89. All Class Members were injured when Aetna caused their PII and PHI to be exfiltrated by cybercriminals.

90. Plaintiff and Class Members entrusted their PII and PHI to Aetna. Thus, Plaintiff had the reasonable expectation and understanding that Aetna would take—at *minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted their PII and PHI to any entity that used Aetna's services had they known that Aetna would not take reasonable steps to safeguard their information.

91. Plaintiff and Class Members suffered actual injury from having their PII and PHI compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII and PHI—a form of property that Aetna obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII and PHI; (d) fraudulent activity resulting from

the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

92. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII and PHI—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII and PHI for nefarious purposes like identity theft and fraud.

93. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

94. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Rougeau's Experience

95. Plaintiff Rougeau first learned of the Breach when she received a notice email (substantially similar to the Notice) from Defendant on or about May 6, 2023.

96. Upon information and belief, Fortra obtained Plaintiff Rougeau's PII and PHI from NationsBenefits Holdings, LLC who Plaintiff Rougeau's health plan, Aetna, used for delivering health services.

97. Shortly after and as a result of the Data Breach, Plaintiff Rougeau experienced a large increase in spam and suspicious phone calls, texts, and emails.

98. Shortly after and as a result of the Data Breach, Plaintiff Rougeau received a letter from a likely fraudster claiming to be the IRS seeking to obtain Plaintiff Rougeau's personal information.

99. Shortly after and as a result of the Data Breach, Plaintiff became aware that hackers had unsuccessfully tried to gain access to her email account approximately 10 times.

100. As a result of the Data Breach and at the recommendation of Aetna and its Notice, Plaintiff Rougeau made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial statements, freezing her credit, and monitoring his credit information.

101. Plaintiff Rougeau has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

102. Plaintiff Rougeau suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII and PHI and/or financial information.

103. Plaintiff Rougeau is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

104. Plaintiff Rougeau has a continuing interest in ensuring that her PII and PHI and financial information, which, upon information and belief, remains backed up in Aetna's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

105. Plaintiff and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to Aetna.

106. The ramifications of Aetna's failure to keep Plaintiff's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

107. According to experts, one out of four data breach notification recipients become a victim of identity fraud.²⁵

108. As a result of Aetna's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII and PHI is used;
- b. The diminution in value of their PII and PHI;
- c. The compromise and continuing publication of their PII and PHI;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;

²⁵ *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/>.

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Aetna and is subject to further breaches so long as Aetna fails to undertake the appropriate measures to protect the PII and PHI in their possession.

109. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to \$1,000.00 depending on the type of information obtained.²⁶

110. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

111. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

112. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.²⁷

²⁶ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

²⁷ "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) <https://krebsonsecurity.com/tag/fullz/>.

113. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

114. The development of “Fullz” packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and other members of the proposed Class’s stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

115. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.

116. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.” Aetna did not rapidly report to Plaintiff and the Class that their PII and PHI had been stolen.

117. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

118. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

119. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII and PHI. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

120. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”²⁸

121. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.²⁹ According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity;

²⁸ *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

²⁹ *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Oct. 21, 2022).

(7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.³⁰

122. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.³¹ The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTCA.

123. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Aetna] allowed users to bypass authentication procedures” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) (“[Aetna] failed to employ sufficient measures to detect unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) (“[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s Inc.*, No. C-4291 (May 20, 2010) (“[Aetna] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization” and “failed to use readily available

³⁰ *Id.*

³¹ *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen>.

security measures to limit access between instore networks”). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Aetna thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

124. The healthcare industry is a prime target for data breaches.

125. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.³² The next year, that number increased by nearly 45%.³³ The following year the healthcare sector was the second easiest “mark” among all major sectors and categorically had the most widespread exposure per data breach.³⁴

126. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by “bad actors.”³⁵

127. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.³⁶ Indeed, when

³² *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), <https://bit.ly/30Gew91> [hereinafter “*Data Breaches Increase 40 Percent in 2016*”].

³³ *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018), <https://bit.ly/3jdGcYR> [hereinafter “*Data Breaches Up Nearly 45 Percent*”].

³⁴ *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

³⁵ *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), <https://bit.ly/3LJqUr6>.

³⁶ *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

compromised, healthcare-related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.³⁷ Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.³⁸

128. The healthcare industry has “emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers.”³⁹

129. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Aetna knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. Aetna also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Aetna’s customers’ patients as a result of a breach. Aetna nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

130. Aetna disclosed the PII and PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Aetna opened, disclosed, and

³⁷ Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), <https://cnet.co/33uiV0v>.

³⁸ *Id.*

³⁹ Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), <https://bit.ly/3x6fz08>.

failed to adequately protect the PII and PHI of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

131. Aetna's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII and PHI of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

132. Aetna's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

133. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

134. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons residing in the United States whose PII or PHI was impacted by the Data Breach—including all persons that received a Notice of the Data Breach (the "Class").

135. The Class defined above is readily ascertainable from information in Aetna's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

136. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Aetna, NationsBenefits Holdings, LLC, and Fortra LLC and their subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Aetna's, NationsBenefits Holdings, LLC's, and Fortra LLC's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

137. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

138. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

139. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately one million individuals whose PII and PHI were compromised by Aetna's Data Breach.

140. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

- a. If Aetna unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

b. If Aetna failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Aetna's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. If Aetna's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Aetna owed a duty to Class Members to safeguard their PII and PHI;

f. If Aetna breached its duty to Class Members to safeguard their PII and PHI;

g. If Aetna knew or should have known that its data security systems and monitoring processes were deficient;

h. If Aetna should have discovered the Data Breach earlier;

i. If Aetna took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Aetna's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Aetna's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Aetna's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Aetna's misconduct;

- o. If Aetna breached implied contracts with Plaintiff and Class Members;
- p. If Aetna was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;
- q. If Aetna failed to provide notice of the Data Breach in a timely manner; and
- r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

141. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Aetna's uniformly illegal and impermissible conduct.

142. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

143. **Predominance**. Aetna has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Aetna's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

144. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Aetna. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

145. The litigation of the claims brought herein is manageable. Aetna's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

146. Adequate notice can be given to Class Members directly using information maintained in Aetna's records.

147. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

148. Aetna has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

149. Plaintiff re-alleges and incorporate by reference paragraphs 1-148 of the Complaint as if fully set forth herein.

150. Aetna required its customers to submit Plaintiff's and Class Members' non-public PII and PHI to receive Aetna's services.

151. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Aetna owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiff's and Class Members' PII and PHI held within it—to prevent disclosure of the information, and to safeguard the information from theft. Aetna's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

152. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Aetna holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would at some point try to access Aetna's databases of PII and PHI.

153. After all, PII and PHI is highly valuable, and Aetna knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and Class Members. Thus, Aetna knew, or should have known, the importance of exercising reasonable care in handling the PII and PHI entrusted to them.

154. Aetna owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

155. Aetna's duty of care to use reasonable security measures arose because of the special relationship that existed between Aetna and patients, which is recognized by laws and

regulations including but not limited to HIPAA, as well as common law. Aetna was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

156. Aetna failed to take appropriate measures to protect the PII and PHI of Plaintiff and the Class. Aetna is morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Aetna had in place were wholly inadequate.

157. Aetna breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII and PHI by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII and PHI.

158. The failure of Aetna to comply with industry and federal regulations evinces Aetna's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

159. But for Aetna's wrongful and negligent breach of their duties to Plaintiff and the Classes, patients' PII and PHI would not have been compromised, stolen, and viewed by unauthorized persons. Aetna's negligence was a direct and legal cause of the theft of the PII and PHI of Plaintiff and the Classes and all resulting damages.

160. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Aetna's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and PHI. Aetna knew or should have known that their systems and technologies for processing and securing the PII and PHI of Plaintiff and the Classes had security vulnerabilities.

161. As a result of this misconduct by Aetna, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII and PHI being disclosed to third parties without the consent of Plaintiff and the Classes

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

162. Plaintiff re-alleges and incorporate by reference paragraphs 1-148 of the Complaint as if fully set forth herein.

163. Under HIPAA, Aetna had a duty to use reasonable security measures to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”⁴⁰ Some or all of the medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.⁴¹

164. Moreover, under HIPAA, Aetna had a duty to render the electronic PII and PHI that it maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.”⁴²

165. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect. And the injuries that Aetna inflicted on Plaintiff and Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services’

⁴⁰ 45 C.F.R. § 164.530(c)(1).

⁴¹ *Id.*

⁴² 45 C.F.R. § 164.304 (defining encryption).

Office for Civil Rights (“OCR”) has pursued enforcement actions against businesses which—because of their failure to employ reasonable data security measures for PHI—caused the very same injuries that Aetna inflicted upon Plaintiff and Class Members.

166. Under § 17932 of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), Aetna have duty to promptly notify “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach” the respective covered entities and affected persons so that the entities and persons can take action to protect themselves.⁴³

167. Moreover, § 17932(a) of HITECH states that, “[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.”

168. And § 17932(b) of HITECH states that, “[a] business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.”

169. Under the Federal Trade Commission Act, Aetna had a duty to employ reasonable security measures. Specifically, this statute prohibits “unfair . . . practices in or affecting

⁴³ 42 U.S.C.A. § 17932(d)(1).

commerce,” including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.⁴⁴

170. Moreover, Plaintiff and Class Members’ injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Aetna inflicted upon Plaintiff and Class Members.

171. Aetna’s duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Aetna are bound by industry standards to protect confidential PII and PHI.

172. Aetna owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII and PHI. Aetna also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Aetna’s Data Breach.

173. Aetna owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Aetna knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Aetna actively sought and obtained the PII and PHI of Plaintiff and Class Members.

174. Aetna breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff’s and Class Members’ PII and PHI. And but for Aetna’s negligence,

⁴⁴ 15 U.S.C. § 45.

Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Aetna include, but are not limited to:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII and PHI;
- b. Failing to comply with—and thus violating—HIPAA and its regulations;
- c. Failing to comply with—and thus violating—HITECH and its regulations;
- d. Failing to comply with—and thus violating—FTCA and its regulations;
- e. Failing to adequately monitor the security of its networks and systems;
- f. Failing to have in place mitigation policies and procedures;
- g. Allowing unauthorized access to Class Members' PII and PHI;
- h. Failing to detect in a timely manner that Class Members' PII and PHI had been compromised; and
- i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

175. It was foreseeable that Aetna's failure to use reasonable measures to protect Class Members' PII and PHI would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII and PHI would result in one or more types of injuries to Class Members.

176. Simply put, Aetna's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit

of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Aetna's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

177. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

178. Plaintiff and Class Members are also entitled to injunctive relief requiring Aetna to, *e.g.*, (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporate by reference paragraphs 1-148 of the Complaint as if fully set forth herein.

180. This cause of action is plead in the alternative to the breach of implied contract theory.

181. Plaintiff and Class Members conferred a monetary benefit on Aetna, by paying money for healthcare services that relied on Aetna to render certain services, a portion of which was intended to have been used by Aetna for data security measures to secure Plaintiff and Class Members' PII and PHI. Plaintiff and Class Members further conferred a benefit on Aetna by entrusting their PII and PHI to Aetna from which Aetna derived profits.

182. Aetna enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Aetna instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members

by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Aetna's failure to provide adequate security.

183. Under the principles of equity and good conscience, Aetna should not be permitted to retain the money belonging to Plaintiff and Class Members, because Aetna failed to implement appropriate data management and security measures that are mandated by industry standards.

184. Aetna acquired the monetary benefit, PII, and PHI through inequitable means in that Aetna failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

185. If Plaintiff and Class Members knew that Aetna had not secured their PII and PHI, they would not have agreed to give their money—or disclosed their data—to Aetna or Aetna's customers.

186. Plaintiff and Class Members have no adequate remedy at law.

187. As a direct and proximate result of Aetna's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII and PHI is used; (3) the compromise, publication, and/or theft of their PII and PHI; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in their possession; and (7) future

expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Aetna's Data Breach.

188. As a direct and proximate result of Aetna's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

189. Aetna should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

190. Plaintiff re-alleges and incorporate by reference paragraphs 1-148 of the Complaint as if fully set forth herein.

191. Defendant required Plaintiff and the Class to provide and entrust their PII/PHI and financial information as a condition of obtaining services from Aetna.

192. Plaintiff and the Class paid money to Aetna in exchange for goods and services, as well as Aetna's promises to protect their protected health information and other PII and PHI from unauthorized disclosure.

193. Aetna promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' PII and PHI would remain protected.

194. Through its course of conduct, Aetna, Plaintiff, and Class Members entered into implied contracts for Aetna to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI and PII and financial information.

195. Aetna solicited and invited Plaintiff and Class Members to provide their PHI/PII and financial information as part of Aetna's regular business practices. Plaintiff and Class Members accepted Aetna's offers and provided their PHI/PII and financial information to Aetna.

196. As a condition of being direct customers/patients of Aetna, Plaintiff and Class Members provided and entrusted their PHI/PII and financial information to Aetna. In so doing, Plaintiff and Class Members entered into implied contracts with Aetna by which Aetna agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

197. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide its PHI/PII and financial information to Aetna, in exchange for, amongst other things, the protection of its PHI/PII and financial information.

198. Plaintiff and Class Members fully performed their obligations under the implied contracts with Aetna.

199. Aetna breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

200. Aetna further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA.

201. Aetna further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Aetna created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

202. Aetna further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

203. Aetna further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

204. Aetna's failures to meet these promises constitute breaches of the implied contracts.

205. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Aetna providing goods and services to Plaintiff and Class Members that were of a diminished value.

206. As a direct and proximate result of Aetna's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

207. As a result of Aetna's breach of implied contract, Plaintiff and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing Aetna to adequately safeguard the PII and PHI of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

- i. prohibiting Aetna from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Aetna to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- iii. requiring Aetna to delete and purge the PII and PHI of Plaintiff and Class Members unless Aetna can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Aetna to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII and PHI;
- v. requiring Aetna to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Aetna's systems on a periodic basis;
- vi. prohibiting Aetna from maintaining Plaintiff's and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;
- vii. requiring Aetna to segment data by creating firewalls and access controls so that, if one area of Aetna's network is compromised, hackers cannot gain access to other portions of Aetna's systems;
- viii. requiring Aetna to conduct regular database scanning and securing checks;

ix. requiring Aetna to monitor ingress and egress of all network traffic;

x. requiring Aetna to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiff and Class Members;

xi. requiring Aetna to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Aetna's policies, programs, and systems for protecting personal identifying information;

xii. requiring Aetna to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Aetna's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Aetna to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Aetna provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons;

D. Enjoining Aetna from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: May 16, 2023

GLANCY PRONGAY & MURRAY LLP

By: /s/Brian P. Murray
Brian P. Murray (CT 25372)
230 Park Avenue, Suite 358
New York, NY 10169
Tel: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**

John A. Yanchunis

Marcio W. Valladares

Ra O. Amen

201 North Franklin Street, 7th Floor

Tampa, Florida 33602

Tel: (813) 223-5505

Fax: (813) 223-5402

JYanchunis@forthepeople.com

MValladares@forthepeople.com

Ramen@forthepeople.com

Counsel for Plaintiff and the Class